Mobile Device and Remote Work Policy

Secure use of mobile devices and remote access at PX.Center

Code:	*POL-SIP-008*
Responsible department:	*Information Security*
Issue date:	*24/06/2026*
Approval authority:	*CISO / CTO*

1. PURPOSE/OBJECTIVE

This policy establishes the mandatory guidelines for the secure use of mobile devices and the practice of remote work at PX.Center, in compliance with control 6.7 of ISO/IEC 27001:2022 (remote work), controls 7.9 (security of assets off-premises) and 8.1 (user endpoint devices), and in alignment with POL-SIP-001 (Information Security Policy).

This document defines the protection rules applicable to laptops, smartphones, tablets, and other assets that access the Organization's information outside its physical premises, in order to preserve the confidentiality, integrity, and availability of information even in remote environments and connections outside the corporate perimeter.

2. SCOPE/APPLICABILITY

This policy applies to all employees, service providers, and third parties who access PX.Center information assets outside the Organization's physical premises, on any authorized corporate or personal device. PX.Center's designation as the reference entity covers the other CNPJs in the group, eliminating the need for a separate document per entity.

Included are mobile computing devices such as laptops, smartphones, tablets, corporate USB media, and IoT devices with external connectivity, as well as all remote access to systems, cloud services, and internal organizational data. The use of personal devices (BYOD) is governed by the specific rules of POL-SIP-012. These provisions apply in conjunction with POL-SIP-001 (Information Security Policy), to which this policy is subordinate.

3. TARGET USERS/AUDIENCE

Executive Board, CISO, CTO, Information Security Lead, IT Infrastructure team, area managers, and all employees, service providers, and third parties authorized to use mobile devices or to remotely access PX.Center information assets.

4. REFERENCE DOCUMENTS

- ISO/IEC 27001:2022 (controls 6.7, 7.9 and 8.1)
- POL-SIP-001: Information Security Policy
- POL-SIP-012: BYOD Policy (use of personal devices)
- POL-SIP-002: Incident Management Policy
- POL-SIP-016: Access Control Policy
- POL-SGI-001: Information Lifecycle Policy
- POL-SIP-013: Acceptable Use Policy

5. GUIDELINES / RULES / CONTROLS

5.1 MOBILE DEVICE PROVISIONING AND MANAGEMENT

Mobile computing devices include laptops, smartphones, tablets, corporate USB media, IoT devices with external connectivity, and any other asset capable of accessing PX.Center systems or information outside the Organization's premises. The provision of corporate devices is the responsibility of the Information Technology department, subject to approval by the employee's direct manager.

Inventory, management, and monitoring of provisioned devices are conducted by the IT Infrastructure team through the corporate endpoint management solution (UEM), and endpoint protection is ensured by the corporate EDR solution. Accessing the Organization's information on a device not inventoried by IT is prohibited.

5.2 SECURE DEVICE CONFIGURATION

All corporate mobile devices must maintain active and up-to-date endpoint protection (EDR), enabled disk encryption, strong authentication, and automatic screen lock. Automatic screen lock is mandatory and must activate after a maximum of 5 minutes of inactivity, with unlocking protected by password, PIN, or biometrics. Operating systems and applications must be kept up to date in accordance with the IT patch policy. The installation of software not authorized or previously evaluated by IT is prohibited.

5.3 USE WHILE TRAVELING AND PROTECTION OF ASSETS OFF-PREMISES

In accordance with control 7.9 of ISO/IEC 27001:2022, the removal and transport of corporate devices requires authorization and registration in the IT inventory. Equipment must be kept in a physically secure location, must not be left unattended in public places, and must not be used by third parties. Employees must prevent unauthorized individuals from viewing information in public environments, and sharing the device with unauthorized persons is prohibited.

Maintenance of a device outside the Organization must be authorized and controlled by IT, and the return of the asset must be recorded with the corresponding removal from the inventory.

5.4 REMOTE ACCESS AND REMOTE WORK

In accordance with control 6.7 of ISO/IEC 27001:2022, remote access to PX.Center internal systems must occur exclusively through secure channels, with mandatory use of corporate VPN combined with multi-factor authentication (MFA). Accessing internal systems via direct connections that do not route through the corporate VPN is prohibited. Authorization for remote work is the responsibility of the employee's direct leadership, and technical enablement of access is carried out by the IT team.

Employees must ensure a private and secure physical environment with adequate connectivity, and the use of third-party devices to access the Organization's data is prohibited.

5.5 DATA PROTECTION AND STORAGE

Sensitive or confidential data must not be stored locally on the device without encryption and without approval from the responsible department. Storing the Organization's documents on unauthorized devices or on non-corporate external media is prohibited. When replacing or disposing of a device, the equipment must be returned to IT for secure formatting and removal from inventory.

5.6 REPORTING LOSS, THEFT, OR INCIDENT

Loss or theft of a mobile device must be reported immediately to security@px.center. Information Security will initiate remote lock or wipe of the device through the corporate endpoint management and EDR solutions. Incidents involving mobile devices or remote access are handled in accordance with POL-SIP-002; when personal data is involved, the dpo@px.center channel is also notified for assessment of LGPD obligations.

5.7 USE OF PERSONAL DEVICES (BYOD)

The use of personal devices to access PX.Center information assets is governed by the specific rules of POL-SIP-012. In the absence of authorization and compliance with the controls of that standard, accessing the Organization's systems and data through personal devices is prohibited.

6. RESPONSIBILITIES

Information Technology (IT) is the department responsible for ensuring compliance with this policy and is accountable for investigating violations of its provisions, with security@px.center as the contact channel for information security matters and dpo@px.center for privacy and LGPD matters. Executive Board approves this policy and provides the resources necessary for its execution. The CISO and CTO approve this policy, define the controls applicable to mobile devices and remote access, and are responsible for its maintenance.

The IT Infrastructure team provisions corporate devices, maintains inventory, management, and monitoring through the corporate endpoint management solution (UEM), and enables remote access via VPN with MFA. The Information Security Lead receives reports of loss, theft, and incidents, initiates remote lock or wipe, and manages incident handling in accordance with POL-SIP-002.

Area managers authorize remote work for their teams, validate the need for device provisioning, and ensure that employees under their management comply with this policy. Employees, service providers, and third parties must comply with the rules of this policy, physically protect the devices in their custody, and immediately report any loss, theft, or incident.

7. RECORDS MANAGEMENT

Records maintained in accordance with this document reside in the following repositories: - Corporate mobile device inventory, including history of provisioning, revocation, maintenance,

and disposal: corporate endpoint management solution (UEM). - Register of authorized remote accesses: under the custody of the IT Infrastructure team. - Endpoint protection events and remote lock/wipe actions: corporate EDR and endpoint management solutions. - Incidents involving mobile devices or remote access: in accordance with POL-SIP-002. - Versions of this policy: SGI document repository.

It is mandatory to preserve the integrity of records, with access restricted on a need-to-know basis, and to keep them available for internal and external SGI audits.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on 23/06/2026, with indefinite validity. The document is reviewed annually or in response to a significant incident involving mobile devices or remote work, a regulatory or compliance change, or the adoption of new technology that affects the controls defined herein. Non-compliance with this policy subjects the offender to the disciplinary measures set forth in PX.Center's internal regulations.

9. ANNEXES

No annexes. Operational records reside in the systems indicated in the Records Management section.

CHANGE HISTORY

Version	Date	Author	Change Description
00	23/06/2025	IT and Cybersecurity Department - IS	Creation and Review
01	24/06/2026	SGI	Recoding to acronym